2011 年中国区
网络安全威胁年度报告

2012/1

目录

2011 年中国区网络安全威胁回顾

年度安全标签：

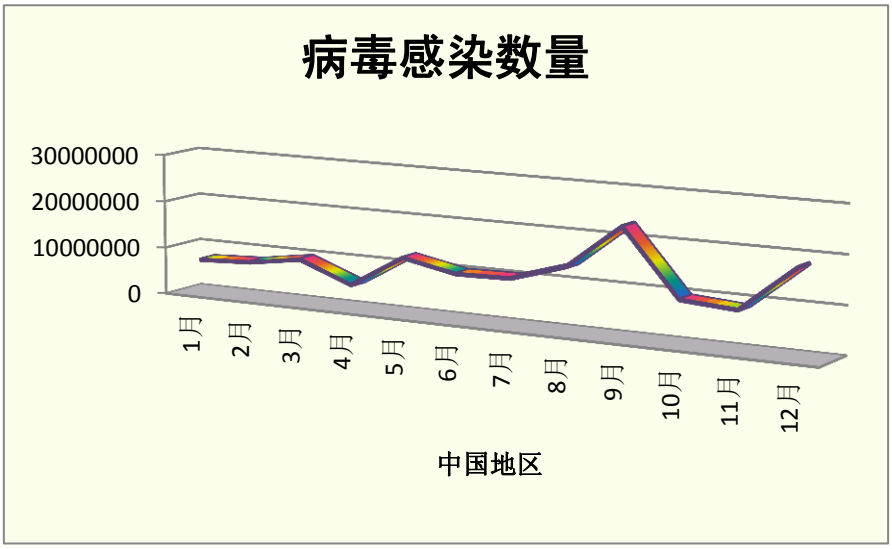
漏洞，具有针对性的病毒与攻击，蠕虫病毒，僵尸网络，手机病毒，跨站攻击。

2011 年度中国区网络病毒回顾

2011 年中国区网络病毒概况

2011 年度趋势科技在中国区发现的新病毒约万种。截止至 2011.12.31 日中国区传统病毒码 8.676.60 可检测病毒数量约为 380 万。

2011 年趋势科技在中国区检测病毒次数约 1 亿 4 千万次。其中 7-10 月为病毒爆发的高峰期。



2011 年中国地区病毒感染情况

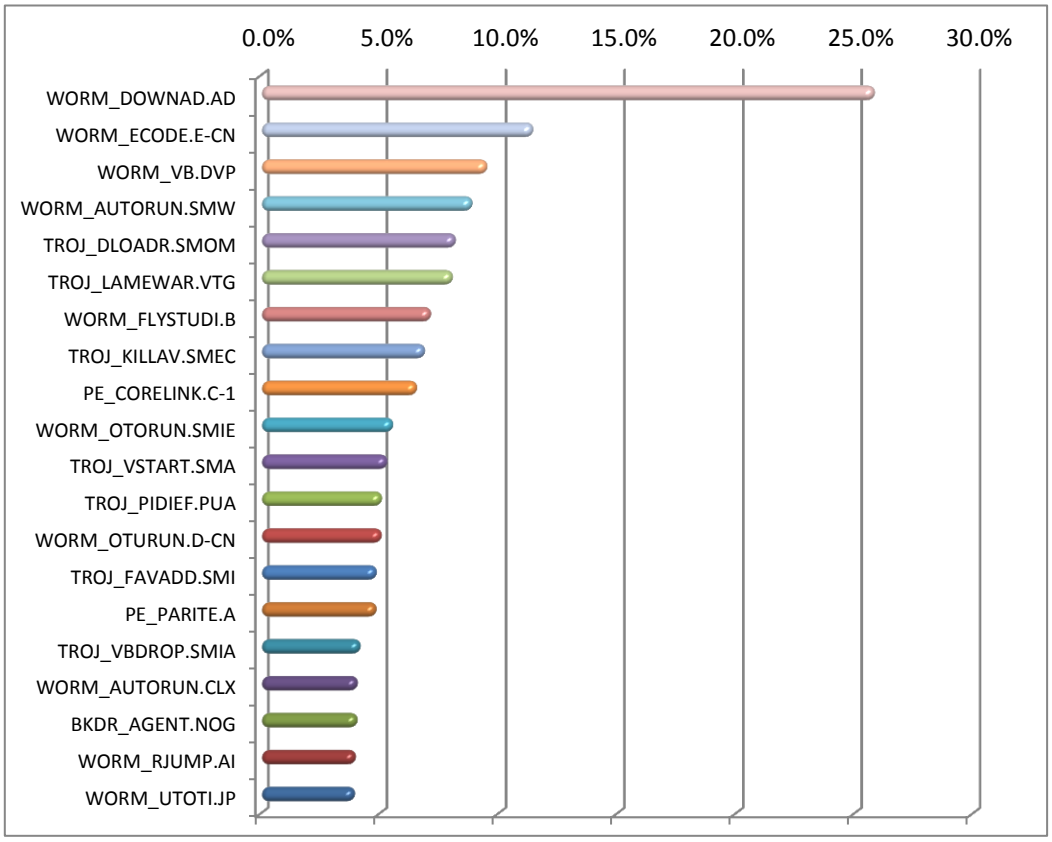
2011 年中国地区网络病毒四宗"最"

2011 年 感染用户最多的病毒

WORM_DOWNAD(飞客) 仍然是今年的“毒王”。作为感染客户数量最多的病毒，WORM_DWONAD 首次出现于 2008 年底，并在 2009 年开始爆发，成功成为 2009 与 2010 年的毒王，而时至今日其仍然存在于很多用户环境中。这支病毒的流行程度在过去的几年无“毒”能及，并且可能在未来的几年都不会被超越。我们认为这种现象与它利用了多个目前普遍存在于网络环境中较难控制的安全弱点有很大的关系。

该病毒主要利用移动存储设备、漏洞、弱密码、以及网络共享进行传播。在这些传播途径中只要有任何一种途径没有进行良好的管理及控制，就会被病毒利用，从而导致病毒大肆传播，无法根除。除非所有企业的安全管理都采用相当规范的模式并严格执行，否则该病毒极有可能在 2012 年继续流行。

由于该病毒在 2011 年并没有新的变种出现，且安全软件对该病毒的查杀手段已经完善，感染该病毒后的查杀工作及后续处理过程不会像前几年那样困难。随着感染此病毒后用户的防范意识提高，该病毒的感染程度及范围必然会呈现下降趋势。



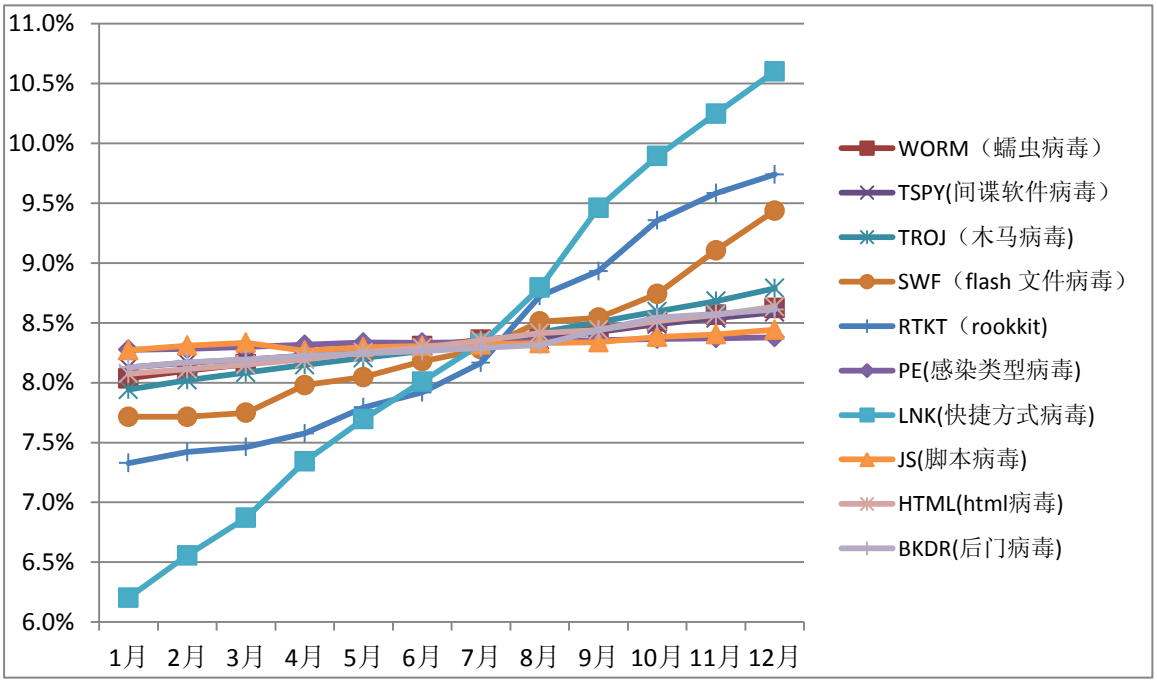
2011 年中国区病毒流行情况

2011 年 增长速度最快的病毒类型

2011 年增长最快的病毒类行为 LNK 类型病毒，这是一种利用了微软操作系统的快捷方式漏洞的病毒。

由于利用了 Windows 的系统漏洞，该病毒的传播能力极强。在存在该漏洞的计算机中恶意程序不需要被手动执行，只要进行浏览操作就会把此病毒激活，并持续感染其他极端及。

由于该漏洞的特性，该类病毒多通过 U 盘等移动存储设备和共享文件夹传播。

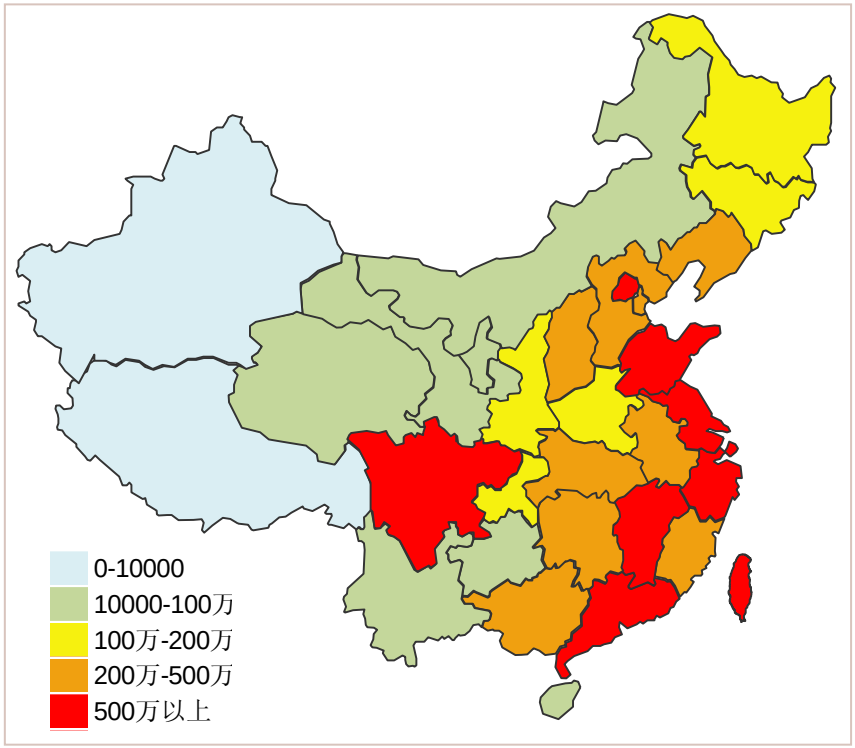


2011 年中国地区病毒增长情况

2011 年感染病毒最多的地区

2011 年中国地区感染病毒最多的地区为：北京，上海，以及广东。从数据中可以发现，除四川之外，病毒感染的高发地区皆为沿海地区。这些地区大都是城市密集的经济发达地区，这些城市工商业发达，电子化程度较高，民众的智能设备普及率及使用率皆较高而民众的日常生活也与这些智能设备密切相关，这种情况成为了病毒传播的良好温床。

随着信息产业的高速发展，网络威胁必将越来越成为企业及个人关心的问题，全国各地的网络安全防范工作也将变得越来越重要。

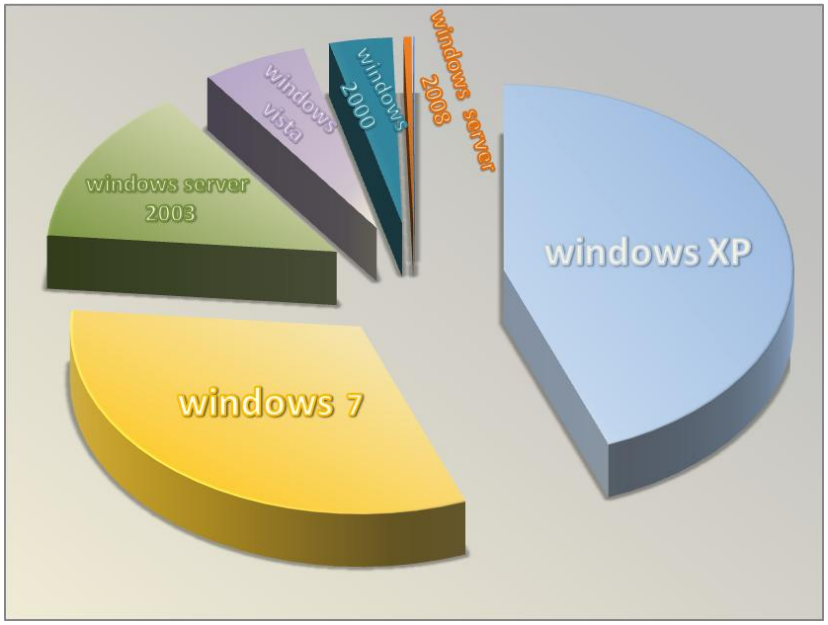


2011 年中国各地区感染病毒情况

2011 年 感染病毒最多的系统

从 2011 年的数据来看，新版的 Windows 操作系统并没有能够成功阻止病毒的传播。在 2010 年底上市的 Windows 7 上的病毒感染数量在 2011 年已经基本与有着十年历史的 Windows XP 齐平，并且隐约有超过 Windows XP 的趋势。当然，该数据结果和 Windows 各个版本操作系统的使用率及面向的用户群体不同有着密切的关系，但是刚上市时消费者“ Windows 7 不会感染病毒”的想法已经可以完全打消了。

Windows 7 虽然采用了多种新技术来加强系统的安全性及可靠性，但也需要安装最新的安全补丁，以及相关防病毒软件，才能够保证安全使用。



2011 年 windows 系统感染病毒情况

2011 年度手机病毒回顾

2011 年对安卓操作系统来说是值得纪念的一年，新版本的陆续发布，功能的不断增强，设备激活量的高速成长，都令人对安卓的未来报以乐观的看法。而对于安卓恶意程序来说也同样如此，安卓操作系统使用者的大量增加让它显得更加有利可图，同时安卓的安全特性也让其更容易成为攻击目标。

安卓系统的病毒多来自于相关的手机论坛，第三方在线软件商店。由于这些论坛以及在线商店没有足够的能力和精力去验证程序包的安全性。因此，这些地方经常出现重新封装过的恶意软件以及盗版软件。

滥用增值服务是 2011 年手机病毒的最大威胁。一旦手机用户不慎感染存在屏蔽业务短信行为的恶意软件，这将让手机几乎成为“聋子”和“瞎子”，任由恶意软件或是通过后台实施恶意扣费等行为；或是自动外拨电话至指定的 SP 业务号码，由于此号段会单独收取高额的 SP 费用，一旦拨打此号码将对用户造成相当程度的资费损失。

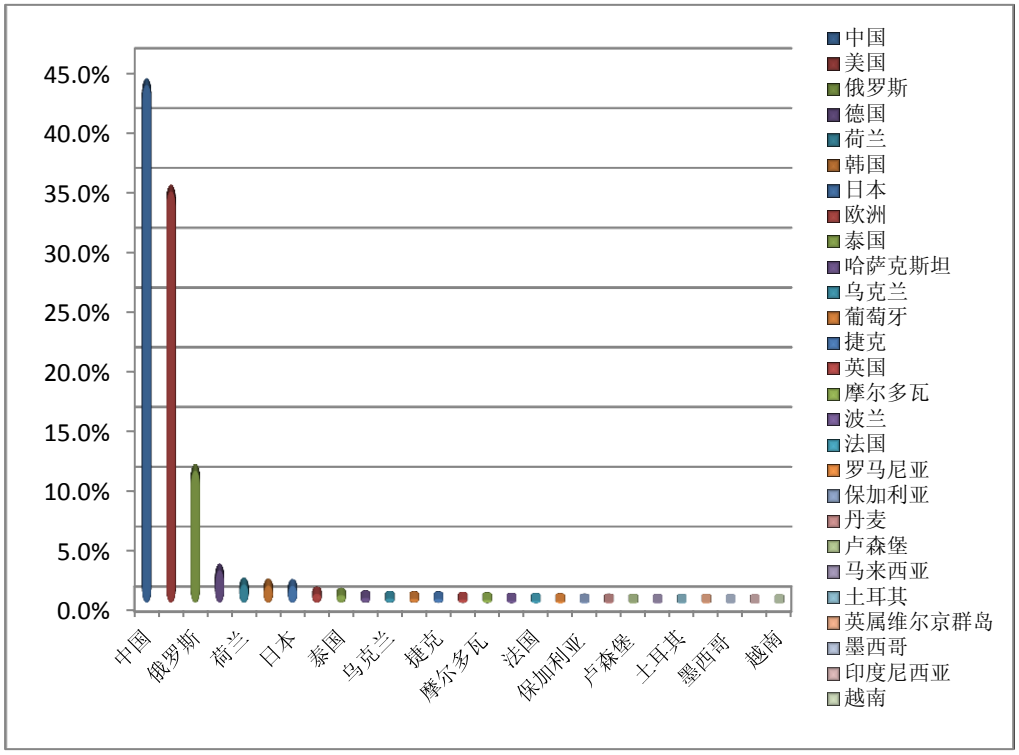
另外，2011 年出现的手机资料外泻的严重事件也是手机恶意程序的杰作。

2011 年度中国区网页安全回顾

2011 年趋势科技在中国地区拦截恶意网页约 400 万次。其中约 10%的网页为被植入恶意代码的正常网站页面，其余的 90%均为恶意网站。

越来越多的恶意网站所有者在国外进行网站域名注册。这一方面可以节约更多的费用，另一方面可以躲过国内的审查机制。

从下图中可以看到，除中国本地外，在美国注册的恶意域名已经占了 35%，超过了中国境外注册的恶意网站数量的一半。



2011 年恶意网站域名所属地

在这些带有恶意程序的网站中，绝大多数为色情网站或赌博类网站。访问该类网站会有很高的感染病毒概率。

被挂马网站中，政府网站占有很大的比例。这说明了很多政府机构缺乏对网站有效地安全管理和维护，使黑客有可乘之机。

2011 年度漏洞与攻击回顾

针对于客户端软件的漏洞情况

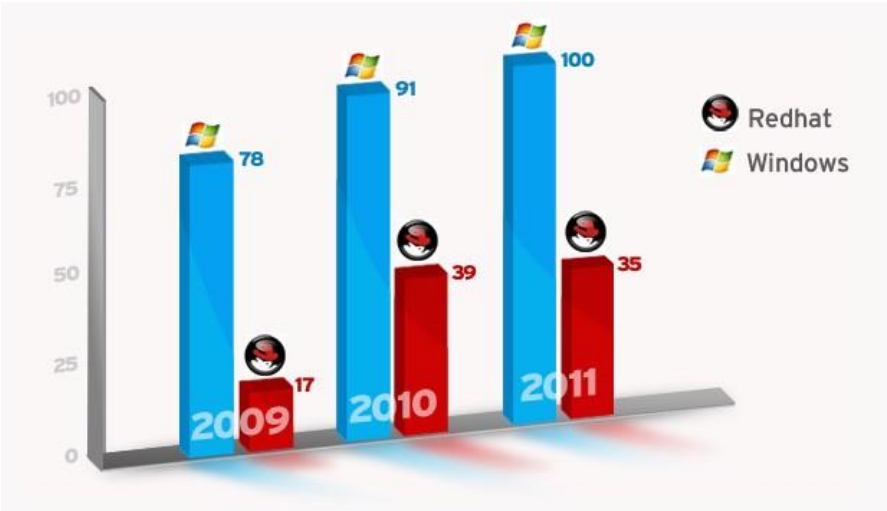
2011 年黑客针对客户端软件的漏洞攻击数量有所增加，并且也变得更加复杂。零日漏洞攻击的数量处于上升趋势。

在 2011 年中，最常黑客攻击的目标软件有 Adobe Acrobat、Adobe Reader、 Adobe Flash Player、Java Runtime Environment(JRE)/Java Development KIT (JDK)以及 Internet Explorer。这些软件的厂商在今年也数次发布相关补丁以修复这些严重的漏洞。

虽然厂商在修补漏洞方面作出了许多努力，但是漏洞攻击仍然有较高的成功率，造成这种情况部分是因为厂商发布补丁不够及时，但更多是因为许多用户在厂商发布补丁后仍没有及时地安装补丁。一份来自 CSIS 的研究报告指出，有 37%的使用者在浏览网页时仍然在使用未经修复的 JAVA。另一份来自 Zscaler 的调查报告也指出 56%的企业使用者用的是有漏洞的 Adobe 版本。

针对于服务器的漏洞情况

2011 年服务器操作系统的漏洞情况也不容乐观。以下显示了 Windows Server 2008 与 Redhat 的漏洞数量。



Windows 与 Redhat 漏洞数量

数据来自 *CVE Details*

此外，由于存在这相当多数量的 Web 服务器，网络犯罪分子也会针对 Web 应用进行漏洞攻击。SQL 注入是最常被利用的攻击手段，2011 年中大约有上百万的 Web 站点被此手段攻破。除了 SQL 注入攻击之外，还有大量其他 Web 攻击发生，例如利用跨站脚本攻击(cross-site script，XSS)、跨站请求攻击（Cross-Site Request Forgery ,CSRF）、跨目录存取（Directory Traversal ），还有其他网页应用程序的漏洞（例如：php .wordpress 和 joomla 等），我们相信在明年也会继续出现这种情况

以下是部分 2011 年影响较为广泛的漏洞：

CVE-2011-0609	Adobe Flash Player ‘SWF’ File Remote Memory Corruption Vulnerability
CVE-2011-3402	Win32k True Type Font Parsing Vulnerability
CVE-2011-3544	Oracle Java SE Rhino Script Engine Remote Code Execution Vulnerability
CVE-2011-2462	Adobe Acrobat and Reader U3D Memory Corruption Vulnerability
CVE-2011-0611	Adobe Flash Player ‘SWF’ File Remote Memory Corruption Vulnerability
CVE-2011-3192	Apache httpd Range Header Remote Denial Of Service

2011 年度中国地区安全威胁大事记

新浪微博 XSS 事件

2011 年 6 月 28 日晚 20 时左右，新浪微博突然爆发“病毒”，大批用户中招，“中毒”用户点击恶意链接后便并自动关注一位名为 hellosamy 的用户，之后开始自动转发微博和私信好友来继续传播恶意地址。不少认证用户中招，也导致该“病毒”被更广泛地传播。

状况持续至 21 时左右，新浪微博官方介入此事件，之后新浪微博在官方微博上发布信息称恶意链接问题得到修复，并表示用户密码等个人信息不会受到影响。据估计，在这期间共有 3w 多名微博用户受到攻击。

根据分析，此“病毒”其实是一个利用了新浪微博的一处漏洞进行的 CSRF 攻击。除了利用漏洞，此次攻击更使用了一些受到广泛关注的话题——如“建党大业中穿帮的地方”、“个税起征点有望提到 4000”、“郭美美事件的一些未注意到的细节”、“3D 肉团团高清普通话版种子”等——来吸引用户的注意。同时，为了节省字符数量而满足微博字符数要求而产生的短域名也为恶意的 URL 2kt.cn 罩上了一层令人无法辨别的 t.cn 的外衣。

通过此次事件可以发现，SNS 作为信息传播渠道，可以快速地传播信息，但如果忽视安全问题，微博将会成为病毒传播的优良渠道。随着各种适应微博这种新型 SNS 形式的各种附加服务地发展，越来越多的新型攻击方式和病毒传播方式将会出现，而原有的一些防范手段的局限性也会越来越大。

Carrier IQ 隐私泄漏事件

2011 年 11 月 12 日，网站 androidsecuritytest.com 出现了一个帖子，，在该帖子中，研究者 Trevor Eckhart 表示，他在他使用的手机上发现了一个名为 Carrier IQ 的预装软件，该软件会在未告知用户的情况下记录用的位置信息和键盘操作。

2011 年 11 月 16 日，Carrier IQ 公司声明称 Trevor Eckhart 为污蔑，并宣称其行为侵犯了 Carrier IQ 的版权。随后 Trevor Eckhart 寻求并获得了电子前锋基金会（Electronic Frontier Foundation，EFF）的支持。随后 Carrier IQ 撤回声明，但依然坚称没有键盘记录等行为。

2011 年 11 月 28 日，Eckhart 公布了一段视频，视频中展示了他所认为的 Carrier IQ 的记录行为，包括键盘操作，浏览记录，短信内容。

此时，该事件已经被越来越多的手机用户关注，随后一些相关运营商及厂商纷纷发表声明。其中 Verizon、T-Mobile、RIM、Nokia 否认他们的设备中安装 Carrier IQ，而 AT&T、Sprint、三星、HTC 承认其手机设备上安装了 Carrier IQ 软件，苹果公司随后也声明已经在 iOS5 的大部分设备中停止了对 Carrier IQ 的支持，而且将会在下一次升级中完全移出该应用。据不完全统计，被安装 Carrier IQ 软件的手机总共超过 3000 万部。单单 Sprint 旗下就有 2600 万台售出的手机安装了 Carrier IQ。

如今，手机的数量已超越传统 PC，并且和人们的日常生活结合得更紧密，同时也存储了更多私人信息和隐私数据。而随着手机智能化的逐步深入，越来越多的手机安全威胁也随之层出不穷。在移动终端，相对于病毒的危害，更多需要关心的是如何将数据安全地存储、应用、传输，从而避免因数据泄漏而给使用者带来的麻烦和困扰。

CSDN 密码泄漏事件

2011 年 12 月 21 日，几乎整个中国的 IT 从业人员都在讨论同一件事：CSDN 用户帐号、密码及邮箱信息被曝，数量超过 600 万。随后又爆出了多家网站密码泄漏的消息。

之后，CSDN 第一时间发布声明向用户道歉，并作出了一定的情况说明。从 CSDN 发布的声明中可以了解到，根据泄漏的用户信息，泄漏时间大约可以定位在 2009 年至 2010 年之间。

自 1999 年 12 月 CSDN 论坛建立至 2009 年 4 月，所有用户密码都是以明文形式保存的。从 2009 年 4 月开始，CSDN 逐步对明文保存的密码进行清理，直到 2010 年 8 月完成所有清理工作，所有明文保存的密码都被销毁，改由加密方式保存，与此同时 CSDN 的用户数量从不到 1000 万逐步增加到了超过 1500 万。

通过对泄漏的信息进行分析后，我们发现的一些触目惊心的数据：
使用纯数字密码的用户超过 289 万；
使用纯小写字母密码的用户超过 74 万；
使用纯大写字母密码的用户超过 3 万；
使用 123456789 做密码的用户超过 23 万；
使用 12345678 做密码的用户超过 21 万；
所有使用弱密码的用户超过 590 万。

而使用足够强度密码的用户不到 9000 人，这些用户的密码都是长度 8 位以上且同时使用大写字母、小写字母、数字且不在常用的密码字典中。

作为站在数字时代网络时代最前沿的程序员群体况且安全意识如此不堪，更何况广大的一般使用者。

再深入挖掘数据后可以发现有超过 40 万的帐号使用生日做密码、有超过 15 万的帐号使用手机号做密码、有超过 25 万的帐号使用 QQ 号做密码，如此，便造成了信息的二次泄漏，导致更广泛的威胁可能性。经过有限地测试，不少帐号的信息可成功登录其他主流门户网站及 SNS，这种 one for all 的密码使用策略会造成大范围的密码失效，并给黑客提供了更有效的密码字典进行破解。

CSDN 并没有公布信息泄漏的途径，但是我们有理由相信，可能的泄漏途径包括网页漏洞、数据库漏洞、系统漏洞、内部人员泄漏、数据或服务器托管商泄漏等。作为一个互联网服务提供者，无疑是“用户越多，责任越大”，在做好服务的同时，更需要将用户的安全放在心上、落到实处。

2012 年网络安全威胁预测

新型的威胁将使用复杂以及高技术的网络犯罪工具以达成目的

APT 先进的持续性渗透攻击(Advanced Persistent Threat, APT)是指针对一特定组织所作的复杂且多方面的网络攻击。APT 攻击者所使用的技术相当先进，同时他们对于目标内部的了解程度也十分深入。APT 可能采取多种手段及渠道，例如恶意软件，漏洞扫描，针对性入侵或利用内部人员破坏安全防护措施。

一般来说具有以下特征的攻击，便可被认定为 APT:

- 出于利益或竞争优势
- 长期持续性的攻击
- 针对一个特定公司，组织或者平台

这种锁定目标的攻击在 2012 年将会不断增长。随着 APT 即网络罪犯之后逐渐为人所知，特定的团体，民间企业，甚至于政府部门都可能使用 APT 手法以达成其目的，而任何一个团体，民间企业，甚至于政府部门也都有可能成为 APT 的受害者。

个人设备(BYOD)的时代来临，将给企业信息安全管理维护带来挑战

许多企业目前仍然在适应 IT 消费化的趋势，但是在 2012 年中我们认为信息安全事故以及资料外泄事件将迫使企业正视个人自备设备(BYOD)将为信息安全维护带来的新挑战。

个人自备设备(Bring-Your-Own-Device,简称 BYOD)的时代已经来临，越来越多的企业资料在知情或不知情的情况下被存储在这些设备上，而 IT 人员却无法管理这些设备，并且这些设备很有可能没有受到充分的保护，从而会进一步导致资料外泻事件不断增加。在 2012 年企业可能将被迫重视个人设备的管理问题，寻找资料保护的最佳方法。

社交网络将成为重要的病毒传播渠道

随着社交网络的发达，年轻的网络社交族乐于在网络上与陌生人分享资料，对隐私权利的重视度相对较低，这让网络犯罪者可以运用社会工程学攻击等手法从中牟利，从 2011 年中知名微博被连续跨站攻击，造成的影响范围之大，我们有理由相信网络犯罪者也从中看到了此平台可能为他们所带来的利益。

智能手机，特别是开源的安卓系统将遭受更多恶意攻击

随着智能手机的普及率不断的升高，预计 2012 年手机平台将会成为网络罪犯的主要攻击目标之一。特别是安卓平台，其自由开放的模式，已经让它成为网络罪犯最爱的攻击目标。这种情况将持续到 2012 年。

截至目前为止，针对移动设备平台的威胁以恶意程序占多数。我们预计未来恶意软件作者会更多利用正常文件中的错误和漏洞，来窃取使用者的资料。由于多数移动设备应用程序开发者对于漏洞的处理与修正流程不够熟悉。这些漏洞一旦被利用，将造成严重后果，修复漏洞的流程也可能会拖得很长。

将会产生更多针对虚拟化以及云服务器的威胁

从目前已知的情况来看，网络罪犯在攻击虚拟平台或者是云平台时，多数仍然采用传统的攻击手法；另一方面，虚拟平台和云平台易被攻击却更难防护。采用虚拟化技术与云技术的同时，安全维护的重担将落在 IT 系统管理员身上，他们一方面必须采用这些新的技术，一方面又需要保护其关键资料不受威胁。但是要修补维护为数众多的虚拟服务器是一项重大的挑战，因此，黑客才会有机会劫持服务器，伪造网络封包，从而入侵含有漏洞的系统并窃取资料。

新型僵尸网络将会流行

由于信息安全产业的反击，网络犯罪的传统工具——僵尸网络(Botnet)——将有规模及形式上的变化。大型的僵尸网络时代将成为历史，取而代之的是更多更小但方便管理的僵尸网络。缩小僵尸网络规模可以降低网络犯罪者的风险，将鸡蛋分散在不同的篮子里面，即便少数网络被取缔，仍有其他僵尸网络可供其进行非法行为。

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC)
本报告部分内容引用自 TrendLab MALWARE BLOG http://blog.trendmicro.com